Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2316005 A1 2002/02/14

(21) 2 316 005

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2000/08/14

(41) Mise à la disp. pub./Open to Public Insp.: 2002/02/14

(30) Priorité/Priority: 2000/08/14 (09/639,434) US

(51) Cl.Int.^{7}/Int.Cl.^{7} H04M 3/22, H04M 1/66

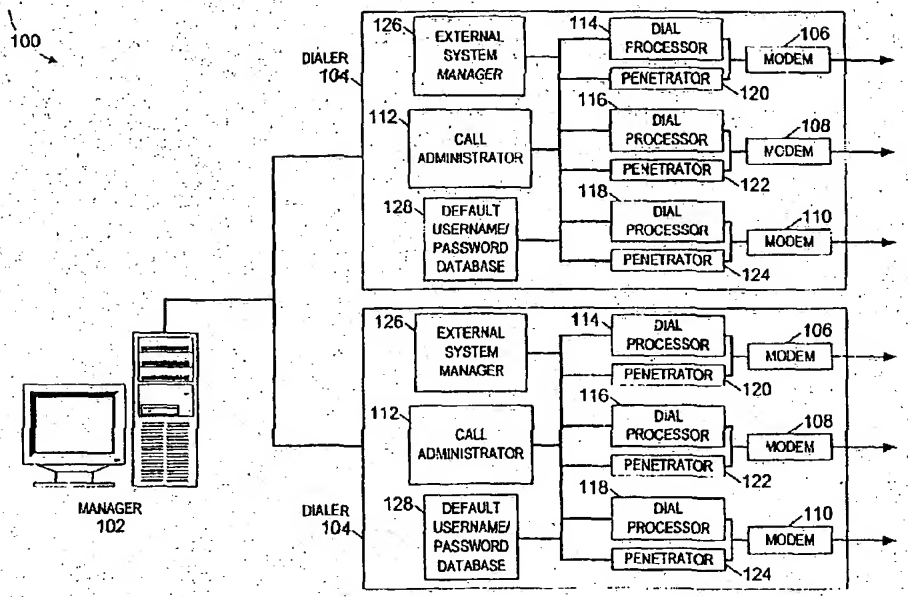
(71) Demandeur/Applicant:
SECURELOGIX CORPORATION, US

(72) Inventeurs/Inventors:
BURGIN, JON, US;
BEEBE, TODD, US

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : METHODE ET SYSTEME AMELIORES D'ESTIMATION DE LA VULNERABILITE DES POINTS D'ACCES PAR LIGNE COMMUTEE

(54) Title: AN IMPROVED SYSTEM AND METHOD FOR DIALUP ACCESS POINT VULNERABILITY ASSESSMENT



(57) Abrégé/Abstract:
A system and method for an automated vulnerability assessment system to more effectively and efficiently identify and assess dialup access points by eliminating operational characteristics associated with unauthorized access attempts is described. The system may include a means for sequenced dialing; a means for uniform time periods between dialing; and a means for multiple calls to the same number in a short period of time, wherein the dialing is performed with autonomous random sequence dialing and varying dialing delays between calls to the same number and multiple low-quantity penetration attempts. The system can also include a means for dialing a range of phone numbers. The system may also include a means for identifying modem and fax carriers. The system may also include a means for identifying the communications application at the terminating station through signature analysis. The system may also include a means for distinguishing between TTY (Teletype) and binary (non-TTY) systems. Additionally, the system can include a means for providing nudge values, and a means for providing a default username and login prompt values associated with a specific system.

AN IMPROVED SYSTEM AND METHOD FOR DIALUP ACCESS POINT VULNERABILITY ASSESSMENT

ABSTRACT

A system and method for an automated vulnerability assessment system to more effectively and efficiently identify and assess dialup access points by eliminating operational characteristics associated with unauthorized access attempts is described. The system may include a means for sequenced dialing; a means for uniform time periods between dialing; and a means for multiple calls to the same number in a short period of time, wherein the dialing is performed with autonomous random sequence dialing and varying dialing delays between calls to the same number and multiple low-quantity penetration attempts. The system can also include a means for dialing a range of phone numbers. The system may also include a means for identifying modem and fax carriers. The system may also include a means for identifying the communications application at the terminating station through signature analysis. The system may also include a means for distinguishing between TTY (Teletype) and binary (non-TTY) systems. Additionally, the system can include a means for providing nudge values, and a means for providing a default username and login prompt values associated with a specific system.

AN IMPROVED SYSTEM AND METHOD FOR DIALUP ACCESS POINT VULNERABILITY ASSESSMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. Patent Application Serial No. 09/312,365 entitled DISTRIBUTED SYSTEM AND METHOD FOR SYSTEM IDENTIFICATION AND VULNERABILITY SCANNING filed May 14, 1999, assigned to the assignee of the present application and incorporated by reference in its entirety.

TECHNICAL FIELD

The invention relates generally to telecommunications access control systems and particularly to a system for dialup access point vulnerability assessment.

BACKGROUND OF THE INVENTION

Security savvy organizations are becoming increasingly effective in protecting computer access to their data networks via the Internet. At the same time, they are acutely aware of the very real and growing threat posed by a lack of security over access to that same data network through their hundreds or even thousands of uncontrolled, unmonitored telephone lines.

In today's high-tech environment, most computer users can easily connect a modem to an existing PC and/or telephone or facsimile line. Once connected, the device effectively bridges the Public Switched Telephone Network (PSTN) to an organization's data network. Each bridge can be thought of as an unmonitored, uncontrolled connection to the Internet, or "untrusted" network.

One of the security professional's worst nightmares is a naïve employee who installs an unauthorized modem and a remote-access program such as pcAnywhere on his workstation without a password (as is most often the case with user-installed modems), and turns on the modem before going home at night. Maybe the employee wants to work at home in the evening or over the weekend, dialing in after-hours to

retrieve files from his hard drive. Or maybe he wants to use the corporate network for free Internet access. Either way, he probably assumes there is little harm in what he is doing—but he has created a serious security breach.

Other less scrupulous individuals might create a similar dialup access point with more malicious intent. Disgruntled employees with authorized access to the data network can perform unauthorized activities from within the private network such as downloading sensitive or proprietary files, or can allow other individuals outside the company to remotely dialup through their system to do the same. This is of special concern in high-security environments where outside transmissions are normally carefully monitored to ensure corporate secrets are not inadvertently or deliberately transmitted.

Crackers, hackers and phreakers know that open modems are an easy target. They use freeware scanners sometimes referred to as "wardialers" to dial a list of telephone numbers, searching for the familiar modem carrier tone. Once the wardialer generates a list of telephone numbers with discovered modems, they dial those numbers looking for an unprotected login or an easily cracked password to a remote-access program. Thus, they gain access to the data network with the potential to steal and/or destroy valuable data behind the front line protection of a firewall.

In a proactive approach to the threat posed by crackers, hackers and phreakers, periodic scanning of an organization's telephone network has become recognized as a necessary component of a corporate security policy. This entails dialing into all of the organization's telephone lines to locate rogue and authorized modems, and then characterizing the security of each device by identifying the operating system/software behind the modem and attempting to penetrate the system in much the same way the bad guys do.

In a defensive effort to prevent unauthorized access, several commercial products targeted by hackers, such as Private Branch eXchange (PBX) systems and remote-access software, now block calls or terminate connection based on calling characteristics that resemble hacking attempts. For example, secure systems resist penetration (hacking) attempts by limiting the number of allowable username and password attempts. If a predefined number of unsuccessful login attempts are made,

the system/software terminates the connection. Also, if multiple unsuccessful login attempts are made to the same account within a short period of time, all connections to that particular account are temporarily prevented for a specified time period.

Another defensive technique used to detect wardialing is for PBX systems to detect the characteristics of calls coming from a particular station. For example, if multiple calls are made with a uniform time between each call, some PBX systems perceive this to be wardialing and automatically block these calls.

Yet another defensive technique PBX systems use to detect wardialing is to observe the progression of numbers being accessed between stations. For example, if the telephone number xxx-xxx0 is called, followed by xxx-xxx1, then xxx-xxx2, this is likely due to some automated dialing appliance. Some PBX systems detect the sequencing of numbers and react to prevent the calls from going through.

Unfortunately, since the characteristics of an organization's security professionals scanning their telephone system looks very much like the characteristics of hacking attempts, the defensive measures mentioned above can be triggered erroneously, causing unnecessary alarms and denial of service.

Additionally, some more clandestine law enforcement and government agencies have an interest in accessing targeted networks without being detected, and without triggering defensive measures similar to those described above.

Clearly, a need exists for a system and method for assessing the vulnerability of dialup access points that is capable of camouflaging its inherent wardialing characteristics.

SUMMARY OF THE INVENTION

The present invention, accordingly, is an automated vulnerability assessment system and method that allows security professionals to more effectively and efficiently identify and assess dialup access points by eliminating operational characteristics associated with unauthorized access attempts. Additionally, the present invention provides a method for identifying non-TTY-based (binary) systems without prior knowledge of the type of system to be penetrated and without the use of the client software.

The present invention is a system that replaces the traditional wardialing characteristics of sequenced dialing, uniform time periods between dialing, and multiple calls to the same number in a short period of time, with autonomous random sequence dialing and varying dialing delays between calls to the same number and multiple low-quantity penetration attempts. The present invention also allows execution of vulnerability assessments without interfering with the security features of other telephony products.

The present invention includes dialing ranges of numbers, identifying modem and/or fax carriers, and attempting to identify the communications application at the terminating station through signature analysis (i.e. matching negotiation signaling and/or textual "banners" to known system types).

The system may generally encounter two types of connections, TTY (Teletype) and binary (non-TTY). Each of these systems transmit unique banners or other data that can be used to recognize the system. A TTY connection is a text-only connection, usually an operating system banner and logon prompt. With a binary connection, a binary protocol is used for handshaking at an application level.

External system objects are usually defined and consist of signatures, nudge values, username and login prompt values, and username/password pairs that are associated with specific systems. A nudge value applies to certain systems that do not answer with a text banner; instead, when a connection is made, these systems wait for the contacting system to provide the nudge value to initiate transactions.

After identifying the communications application at the terminating station, the present invention attempts to establish a connection and test for security vulnerabilities associated with it. If the system is identified, system-specific username/passwords are used in an attempt to login to the system. If the system is not identified, the penetrator uses a list of default username/passwords.

The default username/passwords are common usernames and passwords that are often used as defaults when systems are installed. Many of the username/password pairs that are commonly used as defaults when application or system software is installed. Oftentimes, users do not change these defaults. Because many people know these defaults, any individual could potentially use them to gain

unauthorized access to the network. For example, if the present invention determines it has dialed into a modem on a PC that is running pcAnywhere, it will attempt to gain access to the PC using default pcAnywhere UserID and Password combinations.

One technical advantage achieved with the invention is the ability to autonomously perform multiple login attempts on secure software designed to terminate the connection and deny access if the predefined number of unsuccessful login attempts is exceeded.

Another technical advantage achieved with the invention is the ability to autonomously dial lists of sequential telephone numbers in a random order, thereby avoiding PBX system call blocking.

Another technical advantage achieved with the invention is the ability to autonomously dial the same telephone number multiple times within a short period of time from the same device, but different stations, thereby avoiding PBX system call blocking.

Still another technical advantage achieved with the invention is the ability to automatically dial multiple numbers, with a varying delay time between each call, thereby giving the impression of multiple, random, human-placed calls.

Still another technical advantage achieved with the invention is the ability to autonomously identify and distinguish between TTY-based and non-TTY-based systems without running proprietary non-TTY-based client software.

Yet another technical advantage achieved with the invention is the ability to autonomously identify and distinguish between TTY-based and non-TTY-based systems without prior knowledge of the type of system.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as other features and advantages thereof, will be best understood by reference to the description which follows, read in conjunction with the accompanying drawings wherein:

Fig. 1 is a schematic block diagram of an exemplary vulnerability assessment system of the present invention;

Figs. 2A and 2B are a process flow diagram illustrating the detection avoidance process for the system of Fig.1;

Figs. 3 is a process flow diagram illustrating the determination of eligible numbers to dial process for the system of Fig.1;

Figs. 4A and 4B ~~is~~ are a process flow diagram illustrating the system identification and penetration process for the system of Fig.1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention can be described with several examples given below. It is understood, however, that the examples below are not necessarily limitations to the present invention, but are used to describe typical embodiments of operation.

In Fig. 1, the reference numeral 100 refers to an exemplary vulnerability assessment system of the present invention. The system consists primarily of a manager 102, and one or more dialers 104, interconnected by a Local Area Network (LAN), a Wide Area Network (WAN) or the Internet. The system 100 is capable of providing either local or remote centrally managed enterprise-wide characterization of the organization's telephony security posture.

The manager 102 is the point of user-interface for configuring a dialing profile (rule set), and then pushes the profile to the dialer 104 for execution. Each profile contains a listing of telephone numbers to be dialed and dialing parameters defined for each number or group of numbers.

The dialer 104 has a set of modems 106, 108, and 110, which operate in parallel to perform each dialing task as defined by the manager 102. The dialer 104 also includes a software program, which can be described as one or several entities. For the purposes of this explanation, the software program includes a call administrator 112, at least one dial processor 114, 116, and 118, and at least one penetrator 120, 122, and 124. Each dial processor and penetrator are associated with a modem in this embodiment.

The call administrator 112 maintains the telephone numbers to be dialed, the minimum time delay between calls to the same number, and the random order of the numbers dialed. The dial processor 114 dials the modem 106, establishes connection

with the target modem, pauses for varying lengths of time before making calls, and determines if a call should be torn down (terminated). The penetrator 120 controls the number of penetration attempts per call, the total number of penetration attempts made on a telephone number during the scan, provides salutations and nudges to target systems, recognizes known signatures, responds to prompts from the target system, and performs penetrations.

The dialer 104 also includes an external system manager 126 that manages a collection of system names with corresponding signatures, and where applicable, salutation byte strings and nudges, for use in identifying and penetrating TTY and non-TTY-based systems. The dialer 104 also includes a default username/password database 128 that contains default username/password pairs.

Several configurations are possible, whereby the manager 102 and the dialer 104 are on the same platform for a single stand-alone system, or for large organizations which may be geographically separated, multiple managers 102 and dialers 104 may be interconnected by a LAN, WAN and/or the Internet.

Figs. 2A and 2B are a process flow diagram 200 illustrating the detection avoidance process for the system 100 of this invention. Now referring to Fig. 2A, in step 202, the user configures the dialing profile (rule set) via a management Graphical User Interface (GUI) provided on the manager 102. As part of the dialing profile, the user sets the minimum and maximum time delay between calls to the same number (this random dialing delay prevents the PBX from perceiving the calls as a wardialing attempt). The user sets the maximum number of penetration attempts on a system per call (to avoid the targeted system from locking-out the penetrator 120). The user also sets the maximum number of penetration attempts on a system within the entire scan. A sample profile parameter contains: There will be a random dialing delay of from 10 to 20 seconds between calls, there will be no more than 3 penetration attempts per call, and there will be no more than 10 total penetration attempts on any one system per scan.

In step 204, the manager 102 pushes the profile to the call administrator 112. In step 206, the call administrator 112 applies an algorithm to the phone numbers in the profile, scrambling the order of the numbers.

In step 208, the dial processor 114 requests a number to dial from the call administrator 112.

In step 210, the call administrator 112 determines if there is an "eligible" telephone number available, as discussed below and in further detail later with reference to Fig. 3. If all phone numbers have been called, or if no numbers meet the criteria for elapsed time between calls specified earlier in step 202, the call administrator 112 returns a "null" response in step 212. If a null response is returned, the dial processor 114 delays for a varying amount of time in step 213 prior to requesting another number to dial in step 208. This random delay in requesting a telephone number causes the elapsed time between dialing to be irregular, and therefore appear to not be performed by a dialing appliance, thus avoiding the perception of wardialing.

The dial processor 114 (fig. 1) remains in an active loop, polling the call administrator 112 (fig. 1) for numbers to dial, even when all numbers in the profile have been dialed successfully. In step 210, if the call administrator 112 determines there is an eligible phone number available, the number is provided to the dial processor 114 in step 214.

In step 216, the dial processor 114 dials the number received from the call administrator 112. Once a connection is established with the target system, the dial processor 114 passes control of the call to the penetrator 120.

Now referring to Fig. 2B, the penetrator 120 attempts to identify (if it has not done so previously), and then penetrate the target system in step 218, as discussed below and in further detail later with reference to Fig. 4A and 4B.

In step 220, the penetrator 120 determines if the target system is penetrated. If the system has not been penetrated, the penetrator 120 determines if additional penetration attempts may be made during the current call or subsequent calls in step 222. The decision result is returned to the dial processor 114. If additional penetration attempts can be made during the current call, the dial processor 114 checks to see if a terminating event has occurred in step 224. A terminating event can indicate that the target system has disconnected, or a processing timeout has occurred.

If the dial processor 114 determines that a terminating event has not occurred, the dial processor loops back to step 218 and attempts to penetrate the target system again.

If in step 220, the penetrator 120 determines the target system has been penetrated, or if in step 222, the penetrator determines additional penetration attempts cannot be made during the current call, or if in step 224, the dial processor 114 determines that a terminating event has occurred, the dial processor 114 tears down the call in step 226. In step 228, upon termination of the call, the dial processor 114 sends the call results data to the call administrator 112 where the results are stored. The dial processor 114 loops back to step 213 to wait a random amount of time before requesting another number to dial in step 208.

Fig. 3 illustrates the process 210 whereby the call administrator 112 determines if there is an "eligible" number available for the dial processor 114. In step 300, the call administrator 112 examines the list of telephone numbers in the dialing profile. In step 302, the call administrator 112 compiles a sublist of numbers that are eligible to be dialed with respect to the time of day/day of week, and the minimum amount of time elapsed since the last call, as discussed earlier in step 202.

The call administrator 112 determines if there are eligible phone numbers in the sublist in step 304. If there are eligible phone numbers, the call administrator provide a number to the dial processor 114 in step 306. If there are no eligible numbers to dial, the call administrator 112 provides a "null" response to the dial processor 114 in step 308.

Now, particular reference will be made to Figs. 4A and 4B which illustrate the process 218 whereby the penetrator 120 attempts to identify and penetrate the target system. As previously discussed with reference to Fig. 2A and 2B, the dial processor 114 dials the number, and once the modem 106 is connected, passes control of the call to the penetrator 120. In step 400, the penetrator 120 waits a predetermined amount of time to receive data from the target system. Some systems answer the call with a banner, but other systems wait for the contacting system to provide the proper nudge value to initiate transactions.

If the penetrator 120 does not receive data from the target system during the timeout period, in step 418, the penetrator 120 determines if a nudge is available. If

no nudge is available during the current call, the dial processor 114 assumes control of the call and tears down the call in step 422. In step 424, upon termination of the call, the dial processor 114 sends the call results data to the call administrator 112 where the results are stored. If a nudge is available during the current call, the dial processor 114 assumes control and in step 420, determines if any terminating events have occurred. If no terminating event has take place, the penetrator 120 sends a nudge to the target system in step 426. The system operates in a process loop until data is received from the target system, or until a terminating event has occurred (i.e., run out of nudges, target system disconnects, or timeout for processing).

If data is received in step 400, in step 402, the penetrator 120 requests the external system manager 126 to compare the data against the collection of known system-specific signatures managed by the external system manager 126. In step 404, the external system manager 126 tries to identify the data by comparing it with known system-specific signatures.

If the external system manager 126 matches the data with a signature in the external system manager database, the external system manager 126 then determines if the target system is a TTY-based system in step 406. If the target system is determined to be a non-TTY-based (binary) system, the penetrator 120 implements the appropriate system-specific protocols in step 408. In step 410, the penetrator 120 attempts to penetrate the target non-TTY-based (binary) system by first using system-specific username/passwords, and then using default username/passwords. The penetration process and dialing parameters (number of attempts per call, total number of call backs to the number, etc.) varies as required in accordance with the specific non-TTY protocol.

If in step 404, the data is not identified as a signature belonging to external system manager database, the penetrator 120 examines the last line of the data text to determine if it is an ASCII text prompt (for login, password, username, etc.) in step 412. If the data is ASCII text, the penetrator 120 attempts to penetrate the system using first the system-specific username/password pairs and then the default username/password pairs in step 414.

If the penetrator 120 can not determine that the data is ASCII text in step 412, the penetrator 120 waits for a predetermined period to receive additional data in step 416. If additional data is received during the timeout, the process loops back to step 402 and the penetrator 120 again asks the external system manager 126 to identify the data. If no additional data arrives during the timeout in step 416, the penetrator 120 returns control of the call to the dial processor 114. The dial processor 114 then tears down the call in step 422. Upon termination of the call, the dial processor 114 sends the call results data to the call administrator 112, where the results are stored in step 424.

It is understood that the present invention can take many forms and embodiments. The embodiments shown herein are intended to illustrate rather than to limit the invention; it being appreciated that variations may be made without departing from the spirit of the scope of the invention. The algorithms and process functions performed by the system may be organized into any number of different modules or computer programs for operation on one or more processors or workstations within the system. Different configurations of computers and processors for the system are contemplated. The programs used to implement the methods and processes of the system may be implemented in any appropriate programming language and run in cooperation with any hardware device. The system may be used for enterprises as small as a private business with just a few phone lines as well as for large enterprises with multiple PBX locations around the world. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

CLAIMS

1. An automated vulnerability assessment system to more effectively and efficiently identify and assess dialup access points by eliminating operational characteristics associated with unauthorized access attempts, the system comprising:

means for sequenced dialing;

means for uniform time periods between dialing; and

means for multiple calls to the same number in a short period of time, wherein the dialing is performed with autonomous random sequence dialing and varying dialing delays between calls to the same number and multiple low-quantity penetration attempts.

2. The system of claim 1 further including means for dialing a range of phone numbers.

3. The system of claim 1 further including means for identifying modem and fax carriers.

4. The system of claim 1 further including means for identifying the communications application at the terminating station through signature analysis.

5. The system of claim 1 further including means for distinguishing between TTY (Teletype) and binary (non-TTY) systems.

6. The system of claim 1 further including means for providing nudge values.

7. The system of claim 1 further including means for providing a default username and login prompt values associated with a specific system.

8. A method for automated vulnerability assessment to more effectively and efficiently identify and assess dialup access points by eliminating operational characteristics associated with unauthorized access attempts, the method comprising:

dialing phone numbers in a sequence;

dialing phone numbers with uniform time periods between dialing; and

dialing multiple calls to the same number in a short period of time, wherein the dialing is performed with autonomous random sequence dialing and varying dialing delays between calls to the same number and multiple low-quantity penetration attempts.

9. The method of claim 8 further dialing a range of phone numbers.

10. The method of claim 8 further identifying modem and fax carriers.

11. The method of claim 8 further identifying the communications application at the terminating station through signature analysis.

12. The method of claim 8 further including distinguishing between TTY (Teletype) and binary (non-TTY) systems.

13. The method of claim 8 further including providing nudge values.

14. The method of claim 8 further including providing a default username and login prompt values associated with a specific system.

15. A computer program for automated vulnerability assessment to more effectively and efficiently identify and assess dialup access points by eliminating operational characteristics associated with unauthorized access attempts, the computer program comprising:

instructions for dialing phone numbers in a sequence;

instructions for dialing phone numbers with uniform time periods between dialing; and

instructions for dialing multiple calls to the same number in a short period of time, wherein the dialing is performed with autonomous random sequence dialing and varying dialing delays between calls to the same number and multiple low-quantity penetration attempts.

16. The computer program of 15 further instructions for dialing a range of phone numbers.

17. The computer program of 15 further instructions for identifying modem and fax carriers.

18. The computer program of 15 further instructions for identifying the communications application at the terminating station through signature analysis.

19. The computer program of 15 further including instructions for distinguishing between TTY (Teletype) and binary (non-TTY) systems.

20. The computer program of 15 further including instructions for providing nudge values.

21. The computer program of 15 further including instructions for providing a default username and login prompt values associated with a specific system.

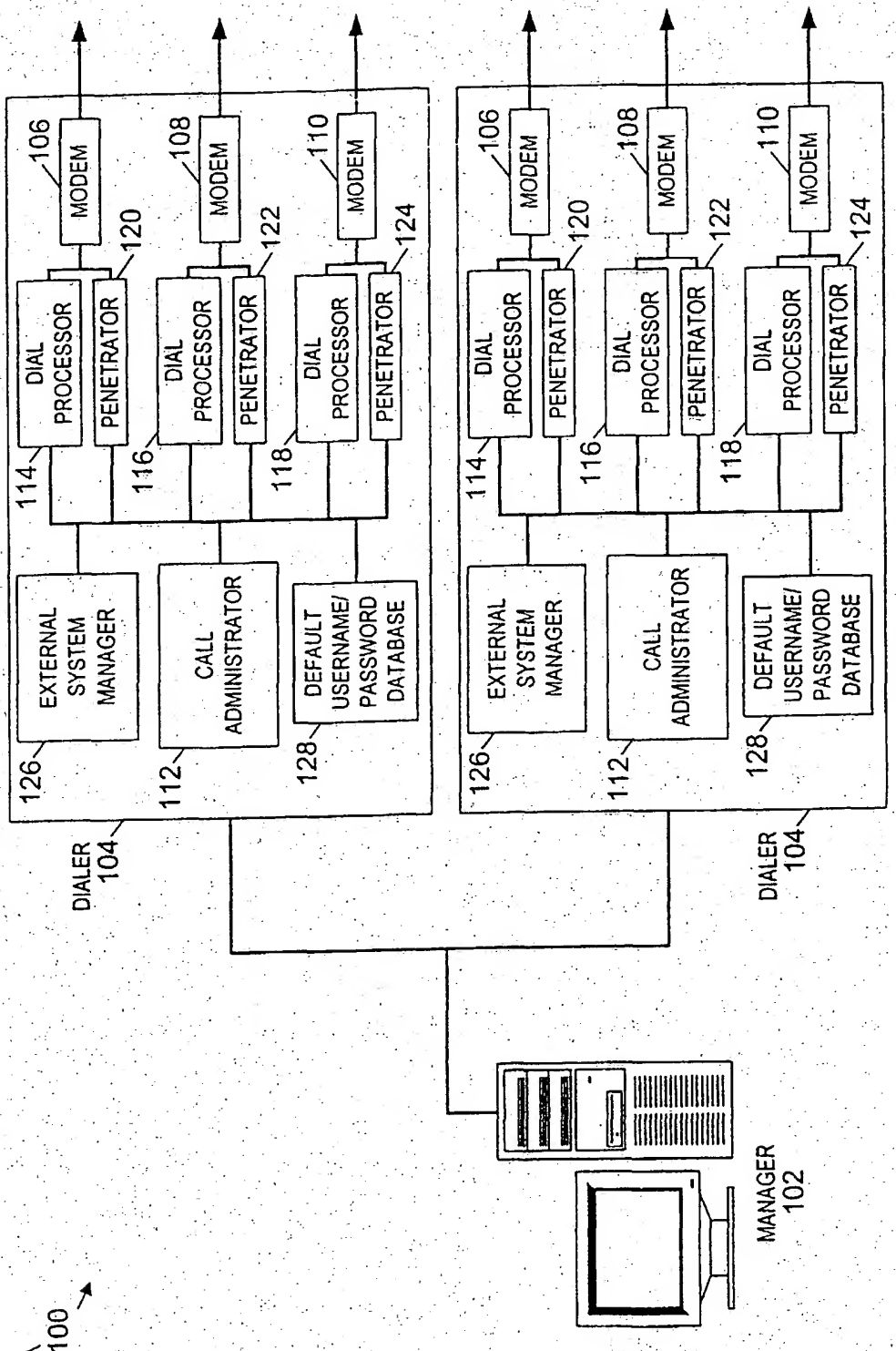

100
MANAGER 102
DIALER 104
DIALER 104
MODEM 106
MODEM 108
MODEM 110
DIAL PROCESSOR
PENETRATOR 120
PENETRATOR 122
PENETRATOR 124
114
116
118
EXTERNAL SYSTEM MANAGER 126
CALL ADMINISTRATOR 112
DEFAULT USERNAME/ PASSWORD DATABASE 128

FIG. 1

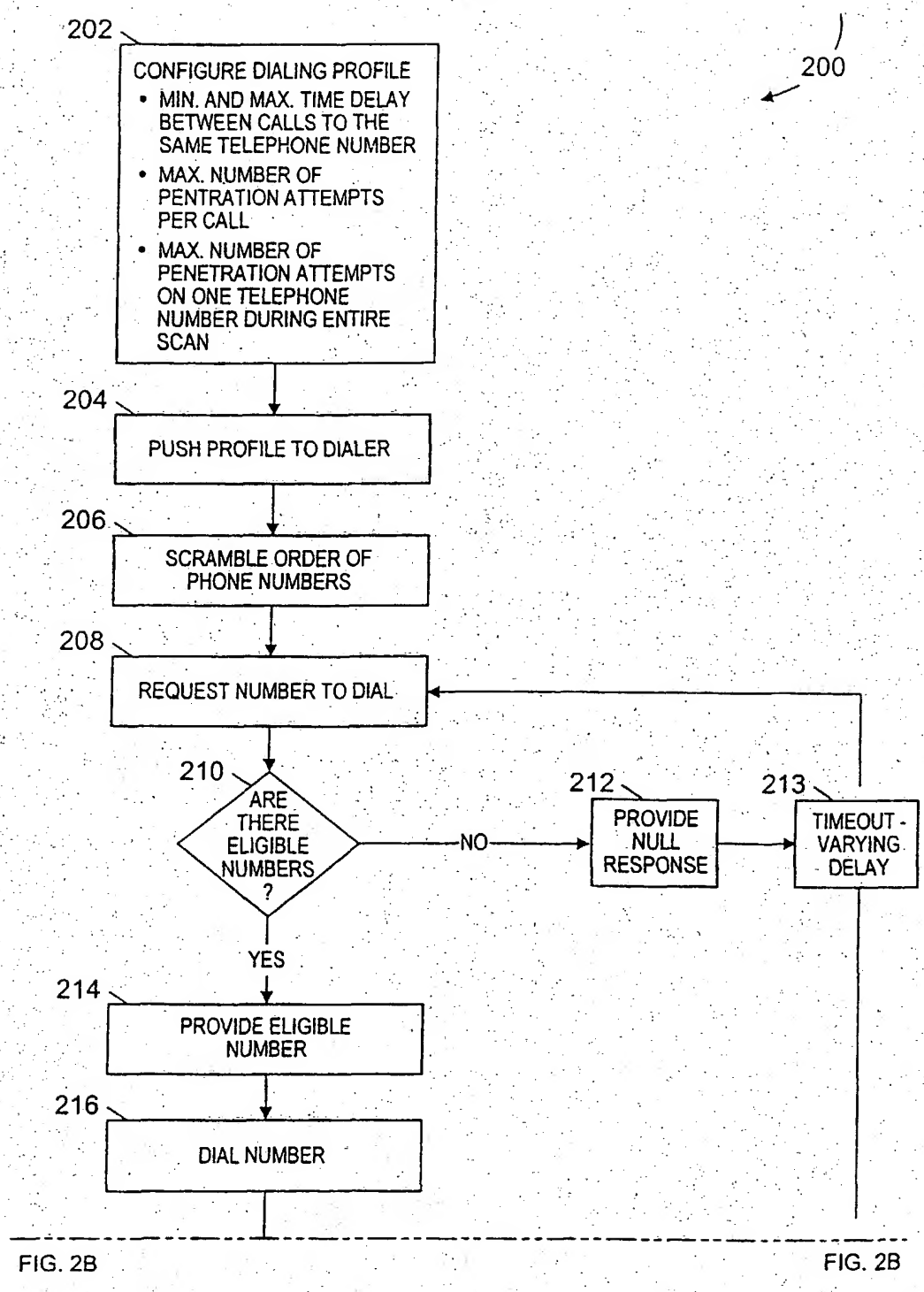

200
202
CONFIGURE DIALING PROFILE
• MIN. AND MAX. TIME DELAY BETWEEN CALLS TO THE SAME TELEPHONE NUMBER
• MAX. NUMBER OF PENTRATION ATTEMPTS PER CALL
• MAX. NUMBER OF PENETRATION ATTEMPTS ON ONE TELEPHONE NUMBER DURING ENTIRE SCAN
204
PUSH PROFILE TO DIALER
206
SCRAMBLE ORDER OF PHONE NUMBERS
208
REQUEST NUMBER TO DIAL
210
ARE THERE ELIGIBLE NUMBERS ?
NO
212
PROVIDE NULL RESPONSE
213
TIMEOUT - VARYING DELAY
YES
214
PROVIDE ELIGIBLE NUMBER
216
DIAL NUMBER
FIG. 2B
FIG. 2B

FIG. 2A

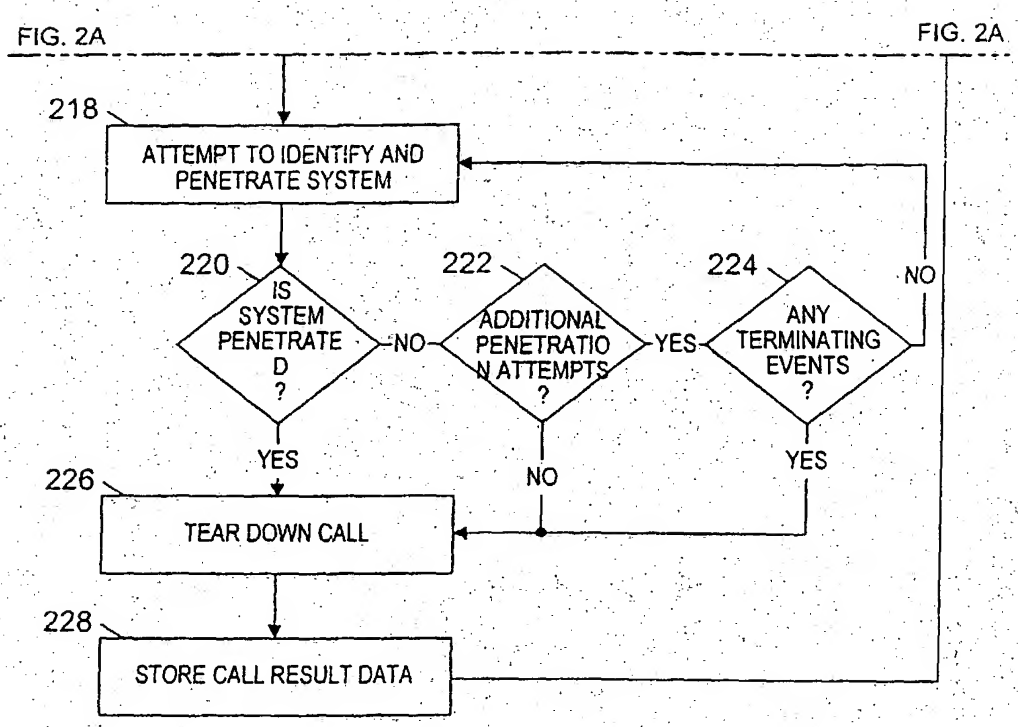


FIG. 2A
FIG. 2A
218
ATTEMPT TO IDENTIFY AND PENETRATE SYSTEM
220
IS SYSTEM PENETRATED ?
NO
222
ADDITIONAL PENETRATION ATTEMPTS ?
YES
224
ANY TERMINATING EVENTS ?
NO
YES
NO
YES
226
TEAR DOWN CALL
228
STORE CALL RESULT DATA

FIG. 2B

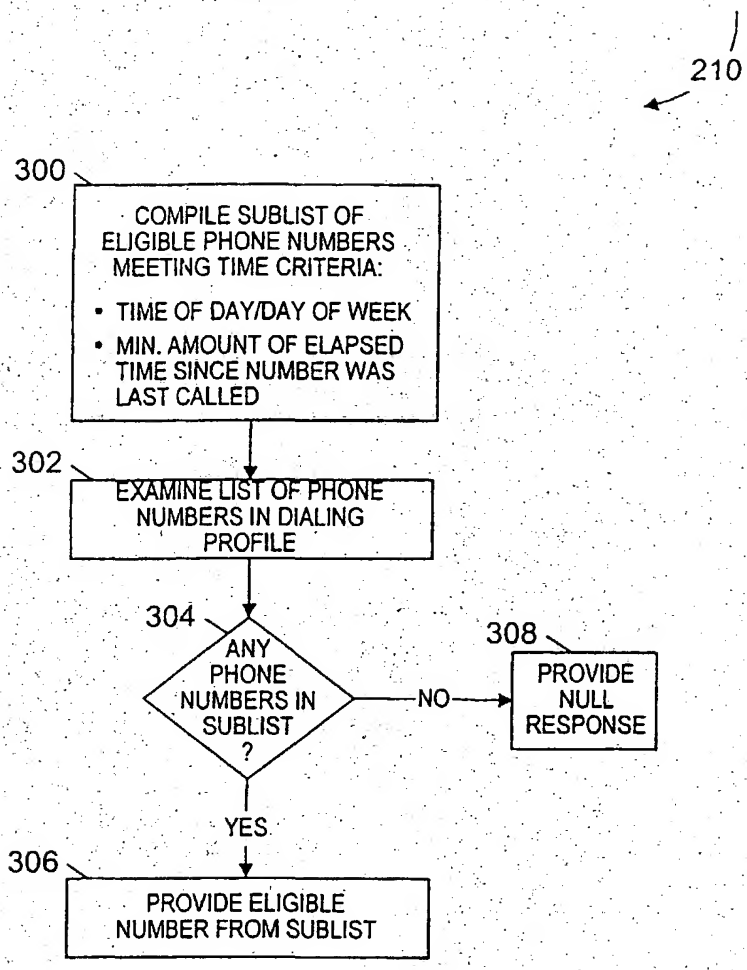

210
300
COMPILE SUBLIST OF ELIGIBLE PHONE NUMBERS MEETING TIME CRITERIA:
• TIME OF DAY/DAY OF WEEK
• MIN. AMOUNT OF ELAPSED TIME SINCE NUMBER WAS LAST CALLED
302
EXAMINE LIST OF PHONE NUMBERS IN DIALING PROFILE
304
ANY PHONE NUMBERS IN SUBLIST ?
NO
308
PROVIDE NULL RESPONSE
YES
306
PROVIDE ELIGIBLE NUMBER FROM SUBLIST

FIG. 3

218

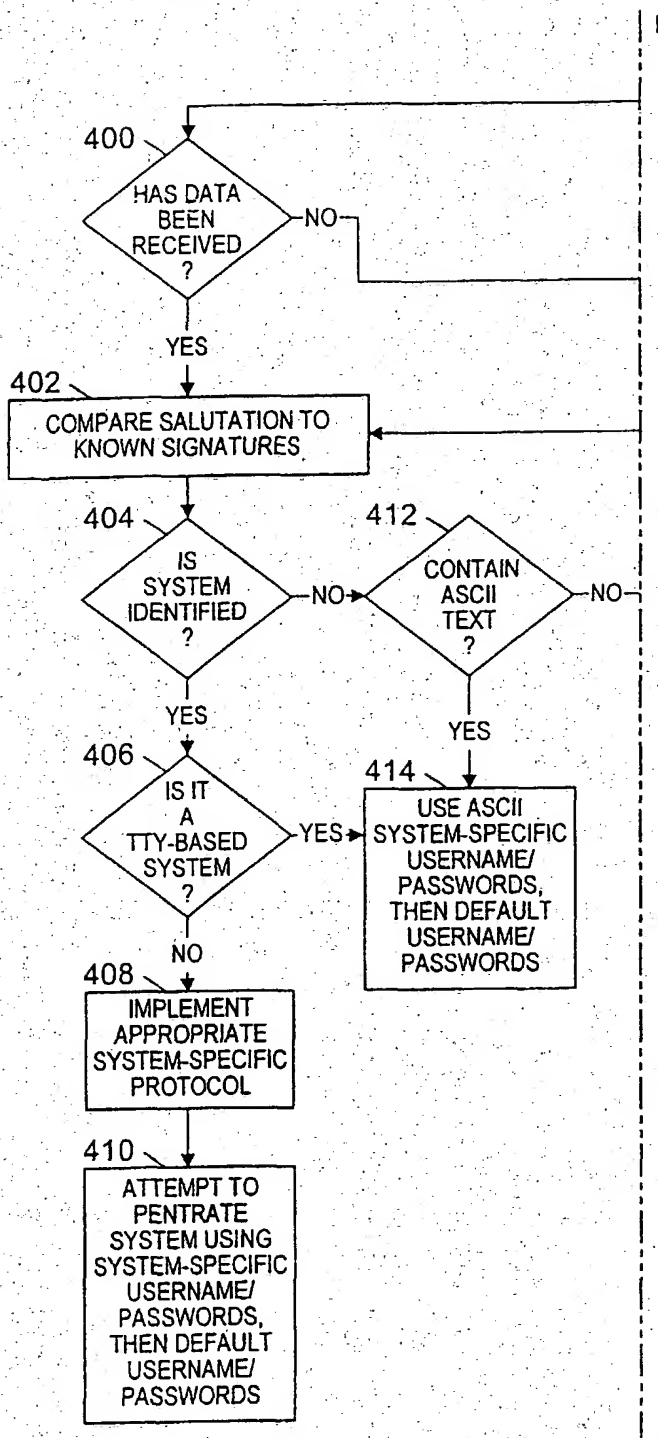


FIG. 4B
400
HAS DATA BEEN RECEIVED ?
NO
YES
402
COMPARE SALUTATION TO KNOWN SIGNATURES
404
IS SYSTEM IDENTIFIED ?
NO
412
CONTAIN ASCII TEXT ?
NO
YES
YES
406
IS IT A TTY-BASED SYSTEM ?
YES
414
USE ASCII SYSTEM-SPECIFIC USERNAME/ PASSWORDS, THEN DEFAULT USERNAME/ PASSWORDS
NO
408
IMPLEMENT APPROPRIATE SYSTEM-SPECIFIC PROTOCOL
410
ATTEMPT TO PENTRATE SYSTEM USING SYSTEM-SPECIFIC USERNAME/ PASSWORDS, THEN DEFAULT USERNAME/ PASSWORDS
FIG. 4B

FIG. 4A

FIG. 4A

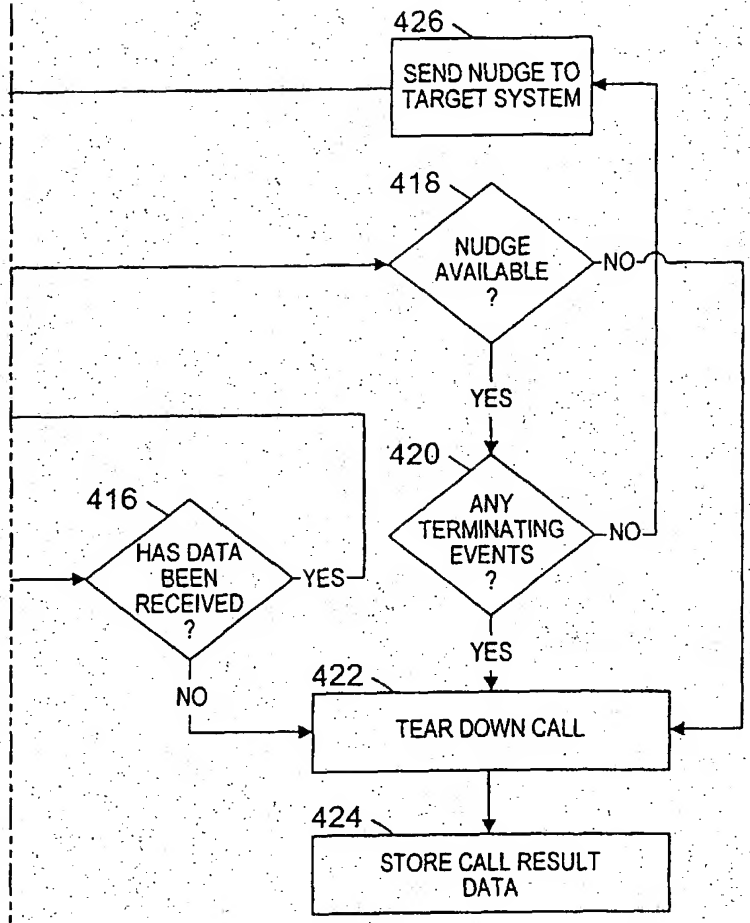


FIG. 4A

FIG. 4B